RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: IDY-W01

Expose and Disrupt: Build Your Attack Paths & Turn the Tables on Attackers

Lindbergh Caldeira

Cyber Security Operations Manager
SA Power Networks
Lindbergh Caldeira | LinkedIn

Ben Cooper

Senior Cyber Security Analyst
SA Power Networks
Ben Cooper | LinkedIn

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

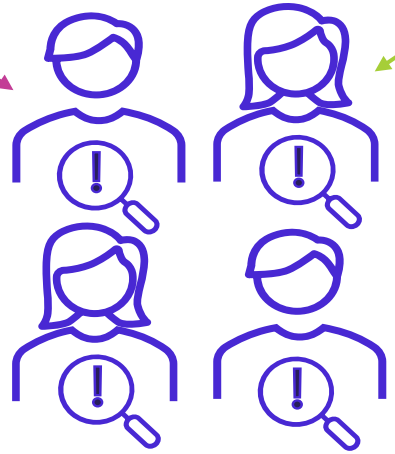
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Day in the life of our SOC team (Before Attack Paths)

Privileged Stale Accounts Alerts

Unauthorised Access Alerts

Vulnerability Management Alerts

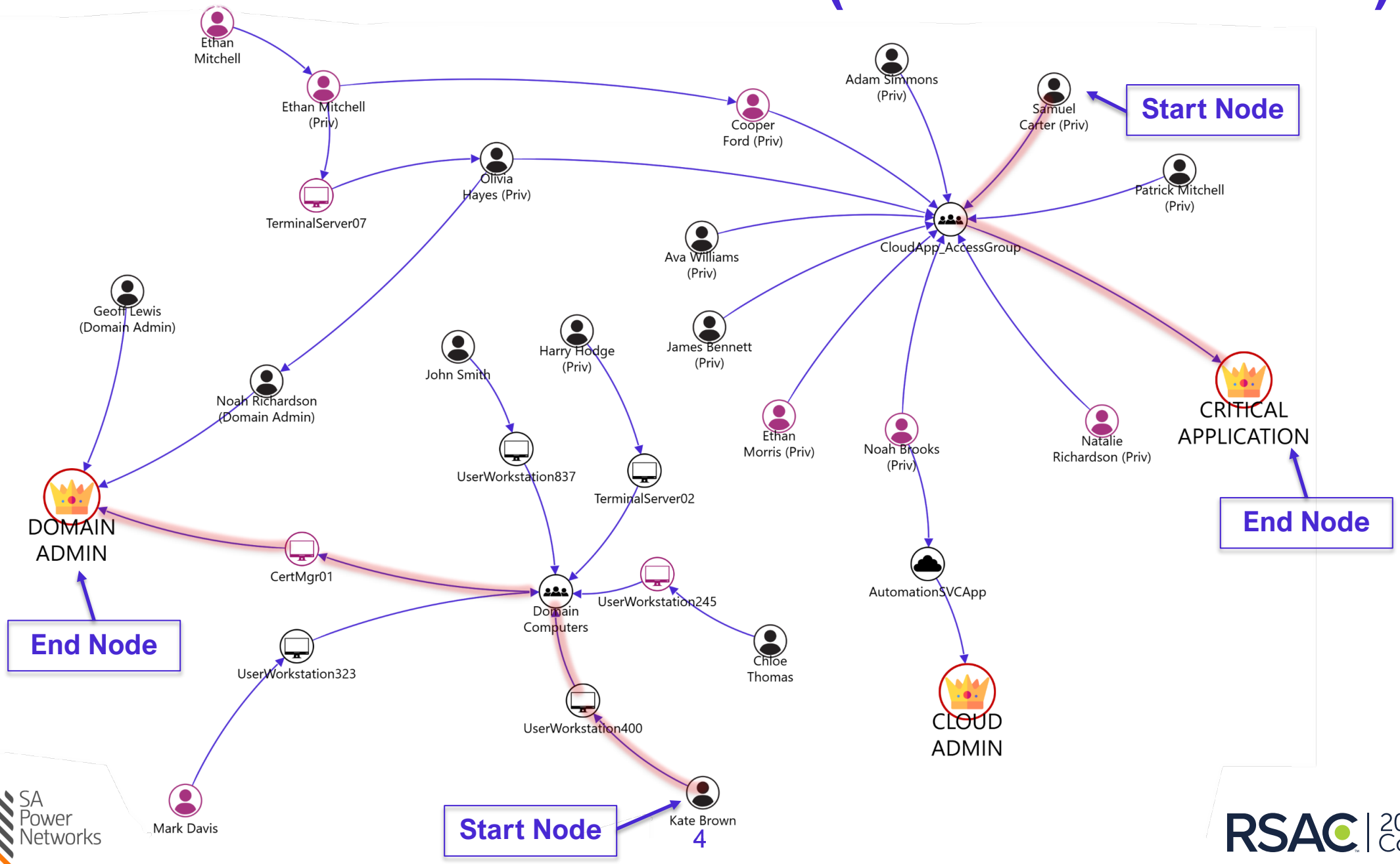


Endpoint Detection & Response Alerts

Phishing Alerts

Compromised and Duplicate Password Alerts

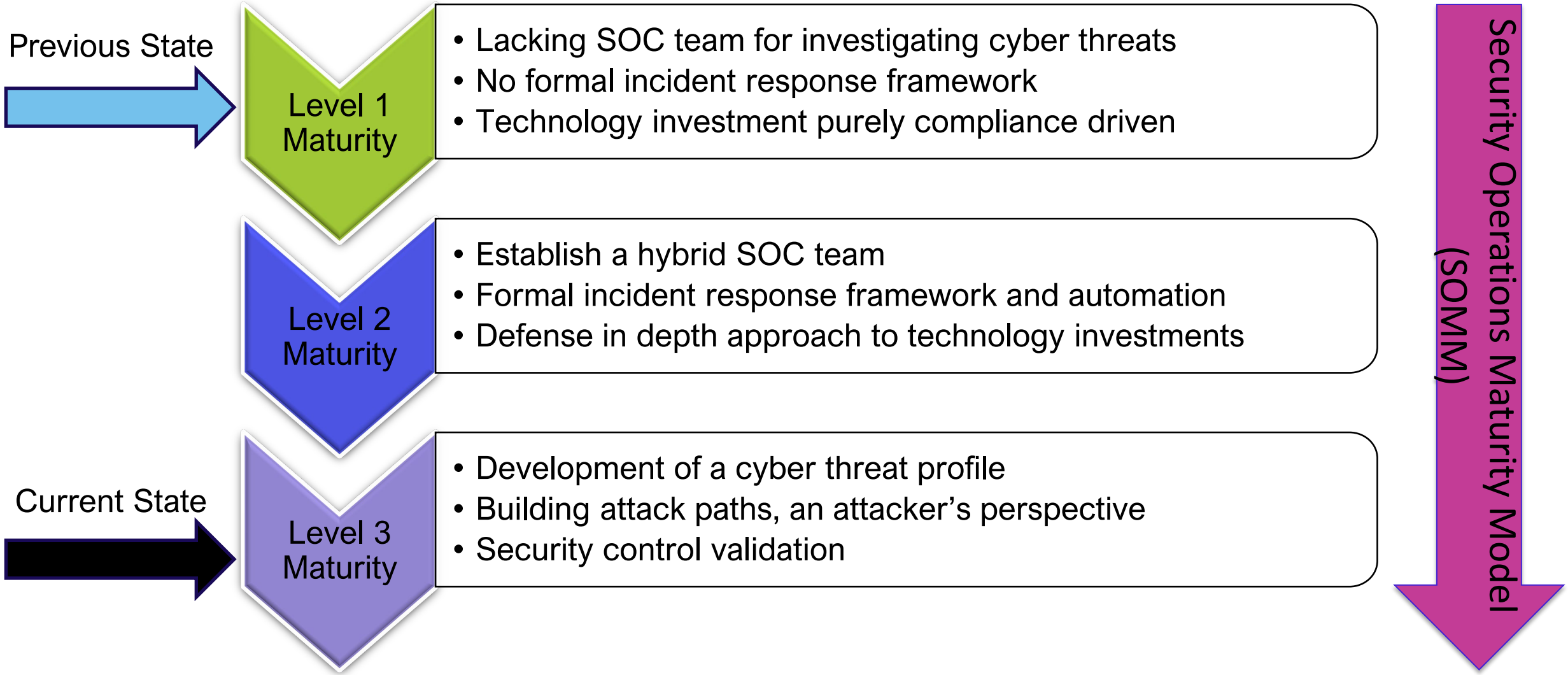
Day in the life of our SOC team (after Attack Paths)



RSAC™ 2025 Conference

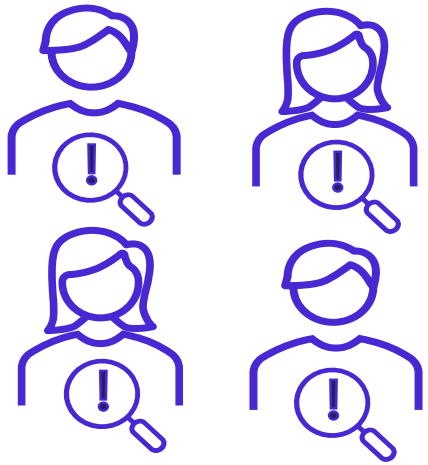
Our SOC Story to Attack Paths

Benchmarking our SOC Maturity

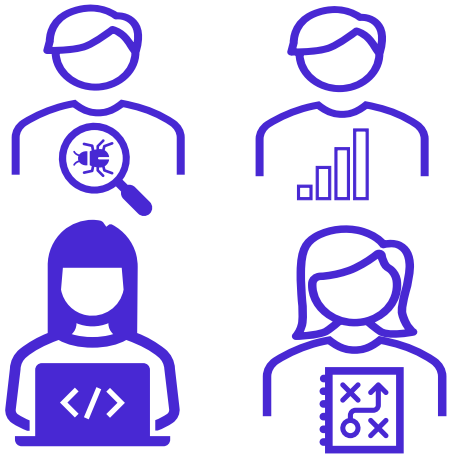

Previous State
Level 1 Maturity
• Lacking SOC team for investigating cyber threats
• No formal incident response framework
• Technology investment purely compliance driven
Level 2 Maturity
• Establish a hybrid SOC team
• Formal incident response framework and automation
• Defense in depth approach to technology investments
Current State
Level 3 Maturity
• Development of a cyber threat profile
• Building attack paths, an attacker's perspective
• Security control validation
Security Operations Maturity Model (SOMM)

Establishing a Hybrid SOC Team

In-House Team

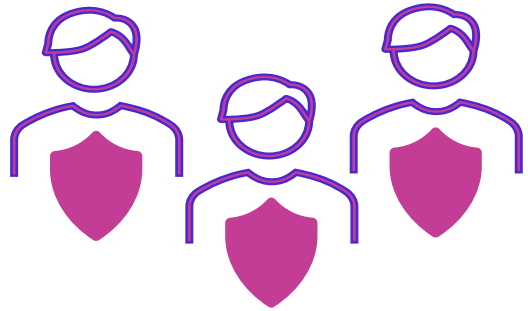


Cyber Security Analysts



Cyber Security Specialists and Engineers

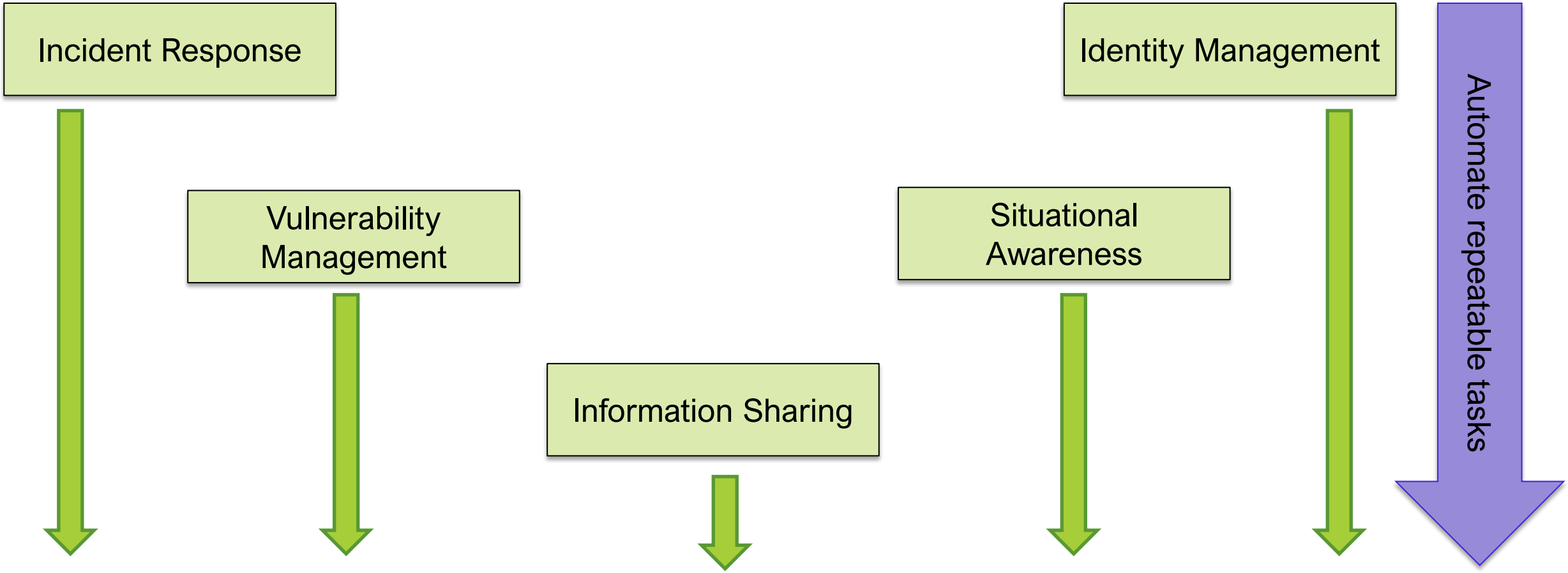
External Services Team



Specialised Detection and Response

Resulted in consistent and timely response to known and unknown cyber threats

SOC Incident Response Framework & Automation



Security Technologies – Defense in Depth

Critical Assets (Customer, Employee, Intellectual Property)

Application (Active Directory, Entra ID, Identity Protection)

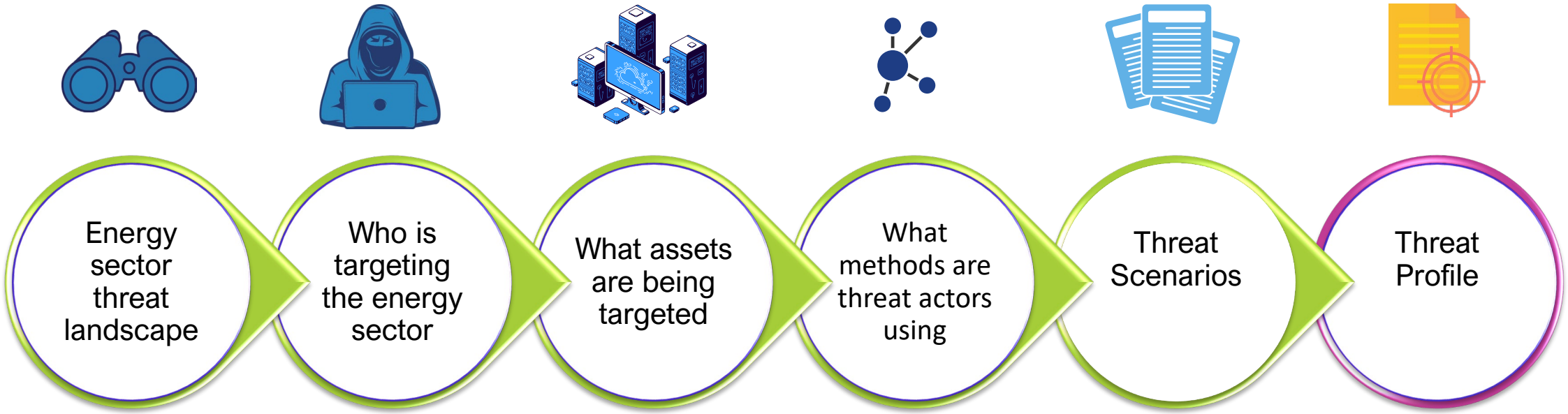
Host (Endpoint Detection & Response)

Internal (Vulnerability Management)

Perimeter (Email Security, Attack Surface Management)

Reduction in potential impact of attacks and proactive threat detection

Building a threat profile

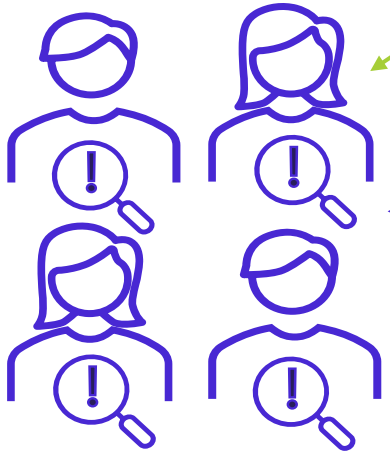

Energy sector threat landscape
Who is targeting the energy sector
What assets are being targeted
What methods are threat actors using
Threat Scenarios
Threat Profile

Bring Us Back to Where We Started

Privileged Stale Accounts Alerts

Endpoint Detection & Response Alerts

Unauthorised Access Alerts



Phishing Alerts

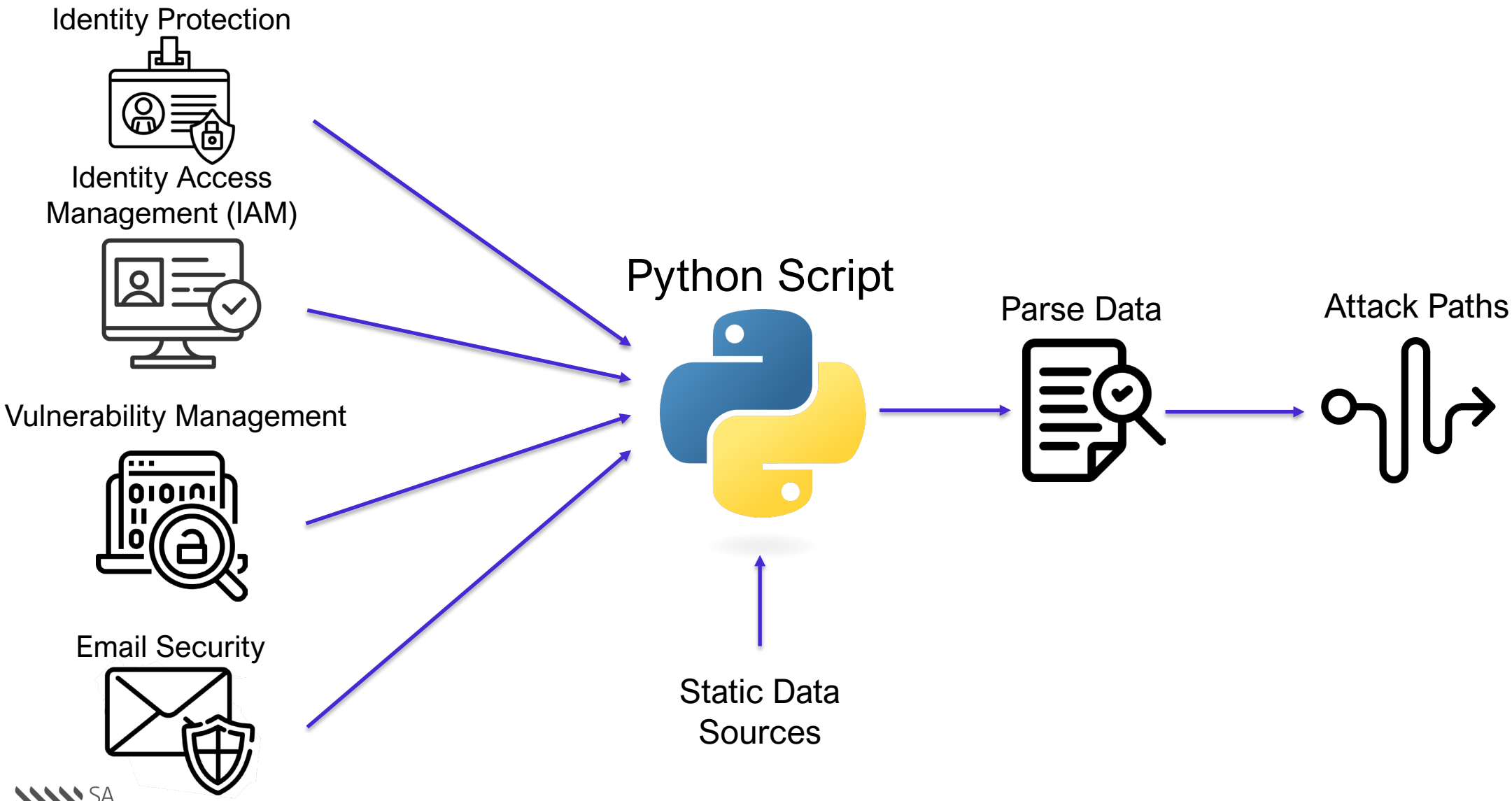
Vulnerability Management Alerts

Compromised and Duplicate Password Alerts

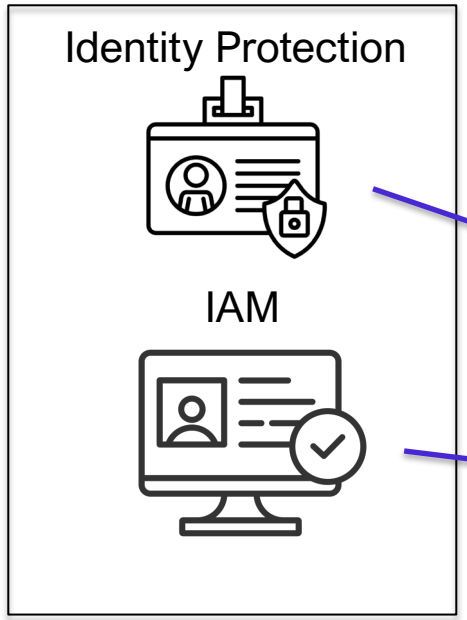
RSAC™ 2025 Conference

Building Attack Paths

Building the Attack Paths: Architecture Overview



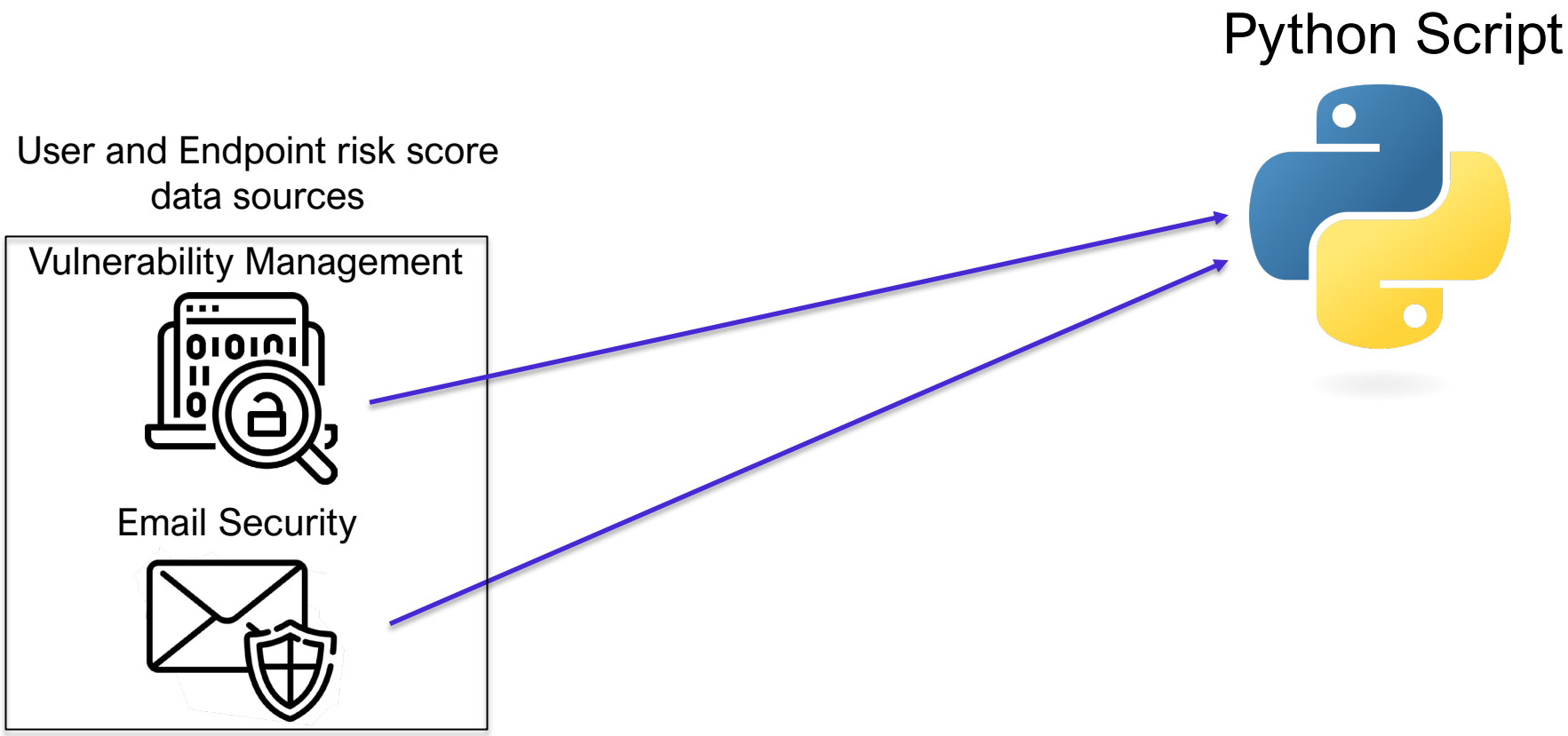
Building the Attack Paths: Collecting the Data



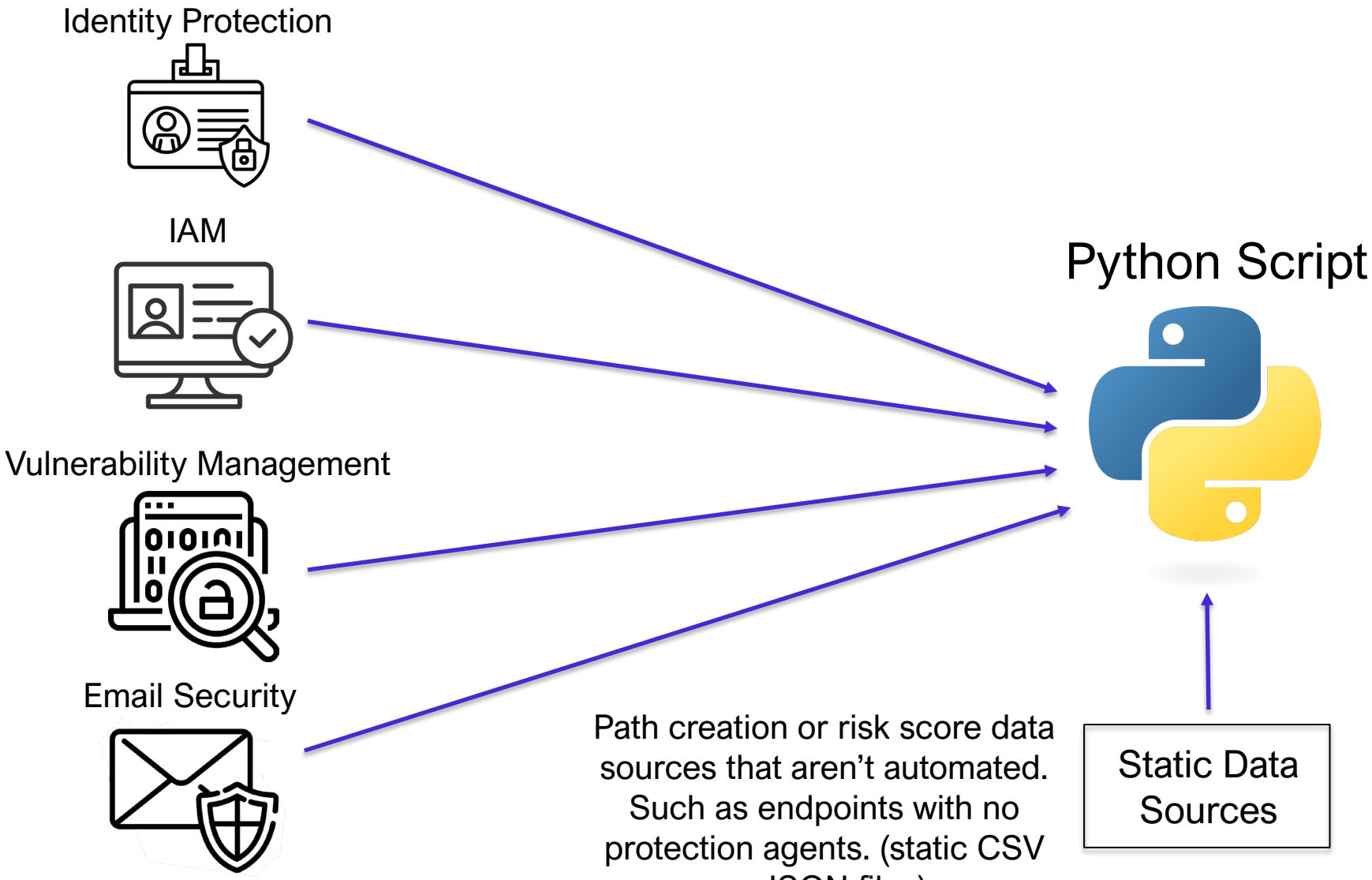
Primarily path creation and node enrichment data sources

Python Script

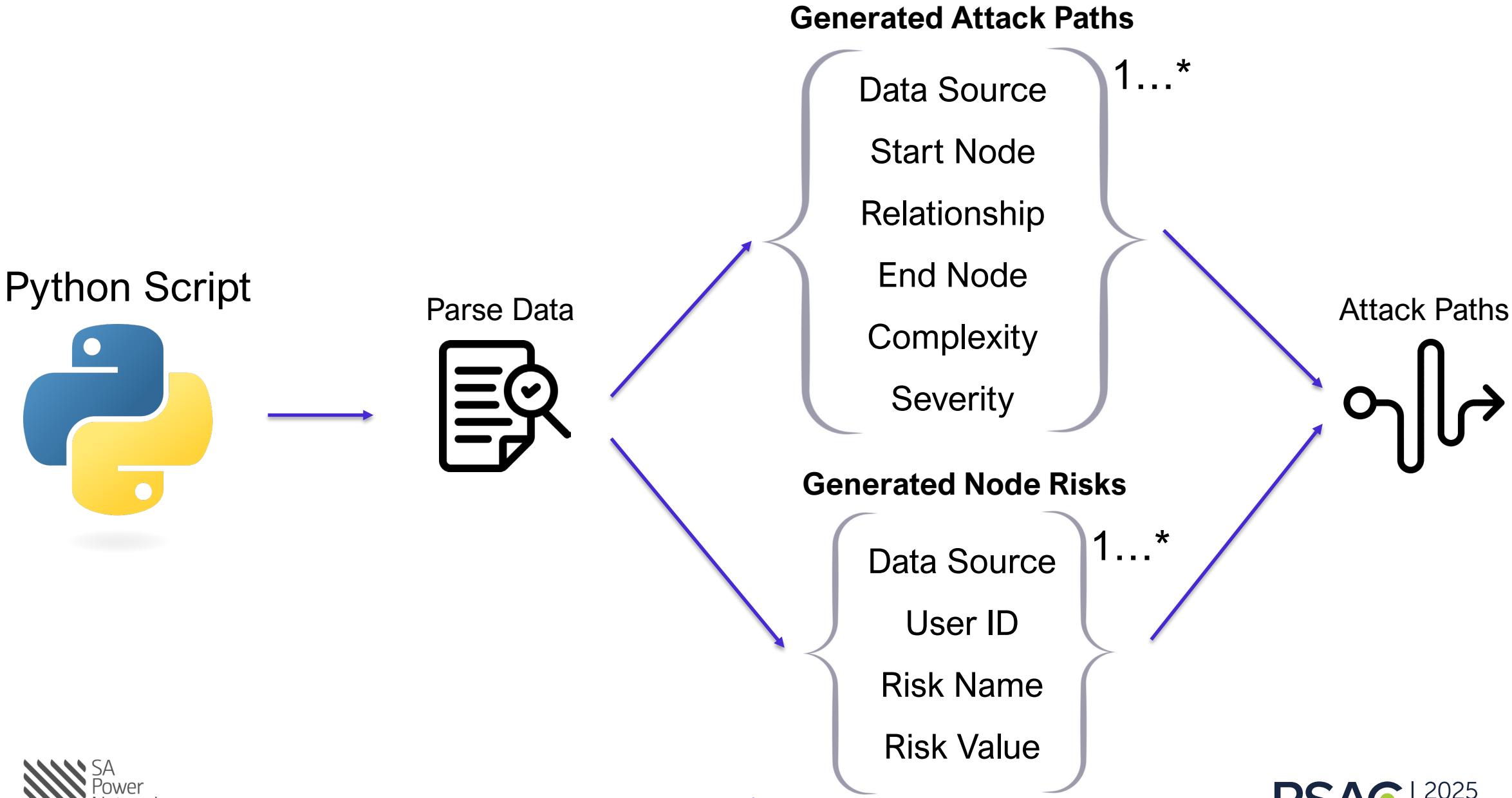
Building the Attack Paths: Collecting the Data



Building the Attack Paths: Collecting the Data

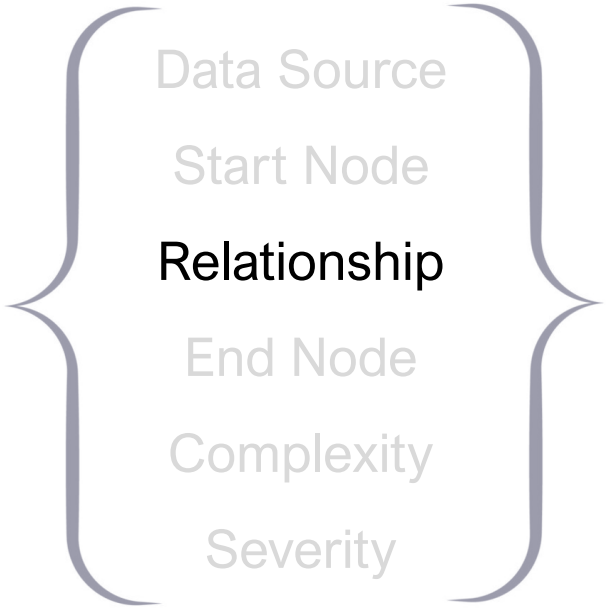

Identity Protection
IAM
Vulnerability Management
Email Security
Python Script
Path creation or risk score data sources that aren't automated. Such as endpoints with no protection agents. (static CSV or JSON files)
Static Data Sources

Building the Attack Paths: Parsing the Data



Building the Attack Paths: Data examples

Generated Attack Paths



Node Relationships Examples

- IN_GROUP
- PASSWORD_RESETTER
- LOCAL_ADMIN
- LOGGED_IN_TO_ENDPOINT
- ADMIN
- DUPLICATE_PASSWORD
- CAN_ACCESS_WITH_SSO

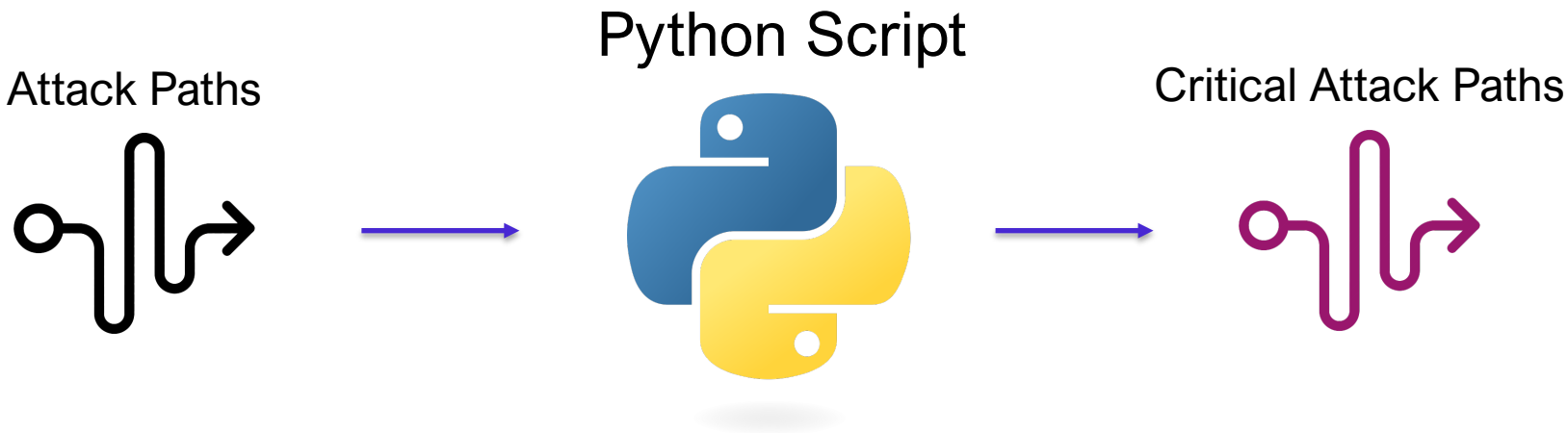
Generated Node Risks

Node Risk Examples

- INACTIVE_ACCOUNT
- MISSING_AGENT
- FAILED_PHISHING_DRILLS
- CRITICAL_VULNS
- DUPLICATE_PASSWORD
- COMPROMISED_PASSWORD

SA Power Networks

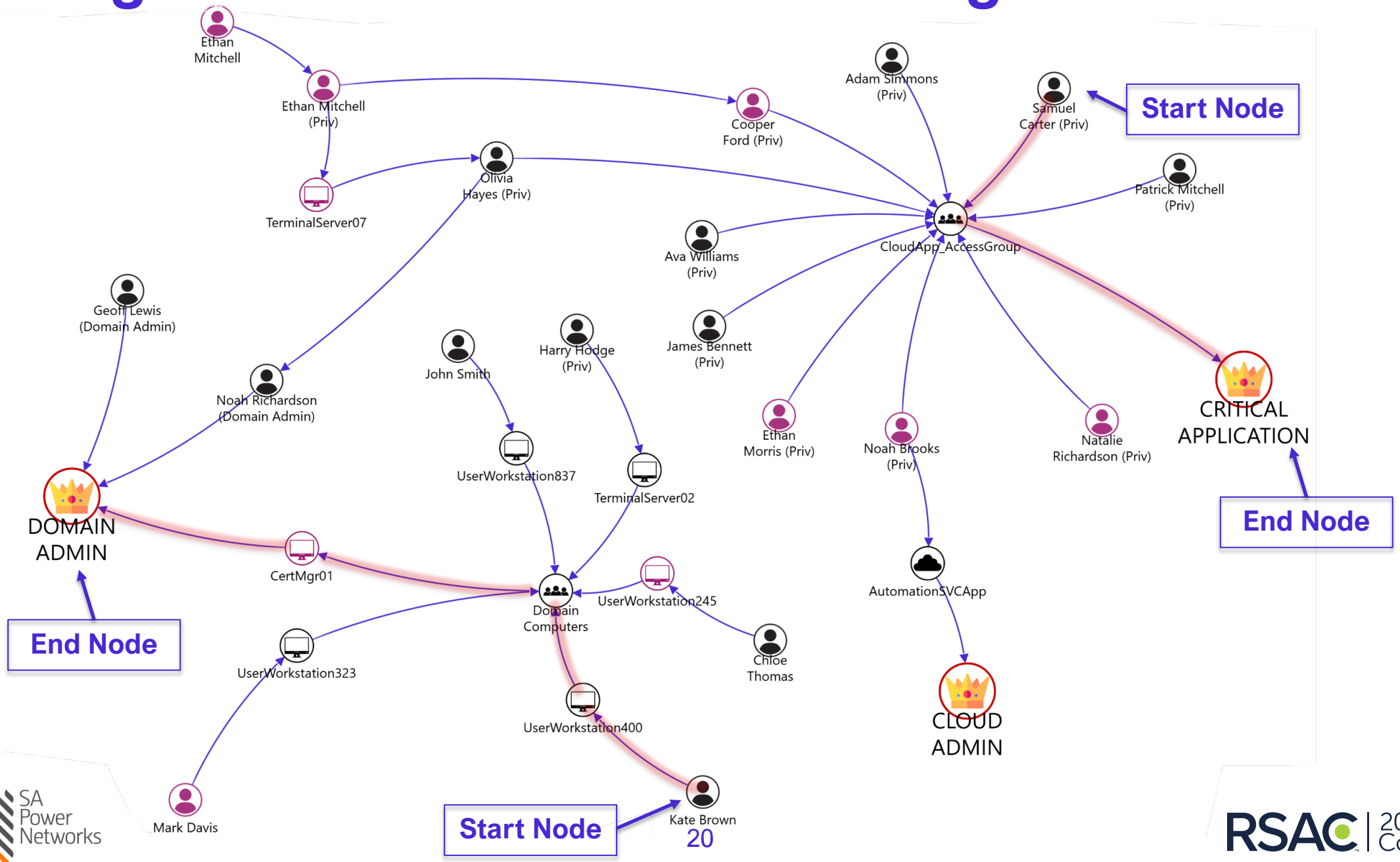
Building the Attack Paths: Prioritising the Paths



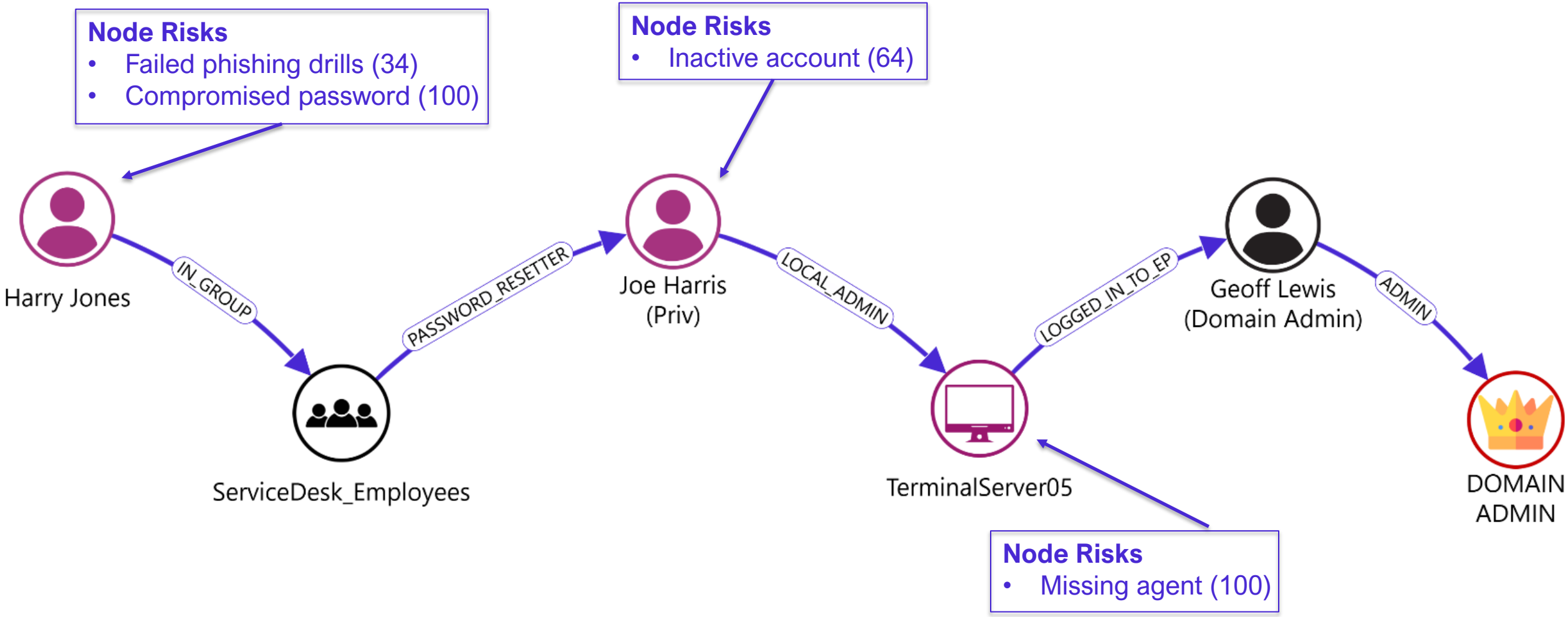
The python script generates the most critical paths based on:

- Associated node risks (e.g. compromised password, missing protection agents, user susceptible to phishing attacks or critical vulnerabilities on assets)
- Number of hops required to reach “End node”
- Complexity of node relationships

Building the Attack Paths: Visualizing the data



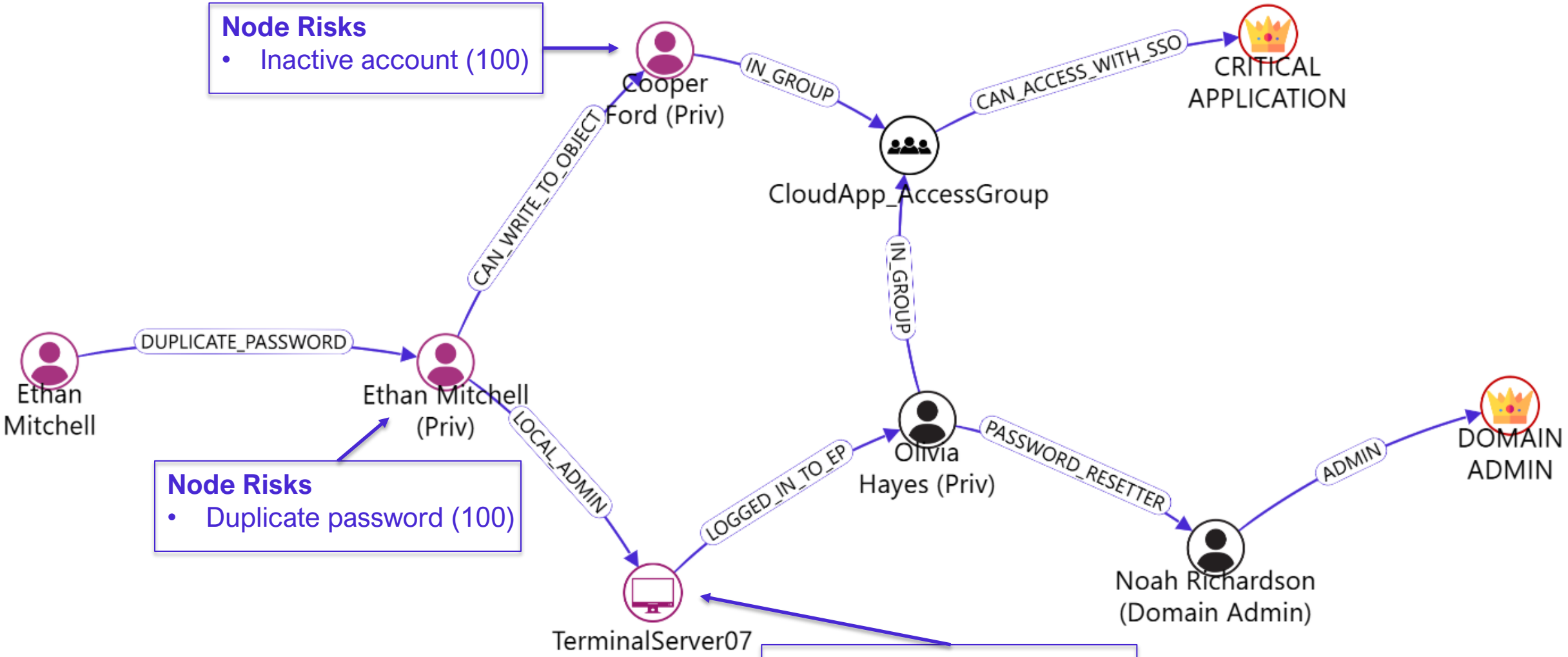
Use Case 1: Easy Win



NOTE: Data is simulated for presentation purposes

SA Power Networks

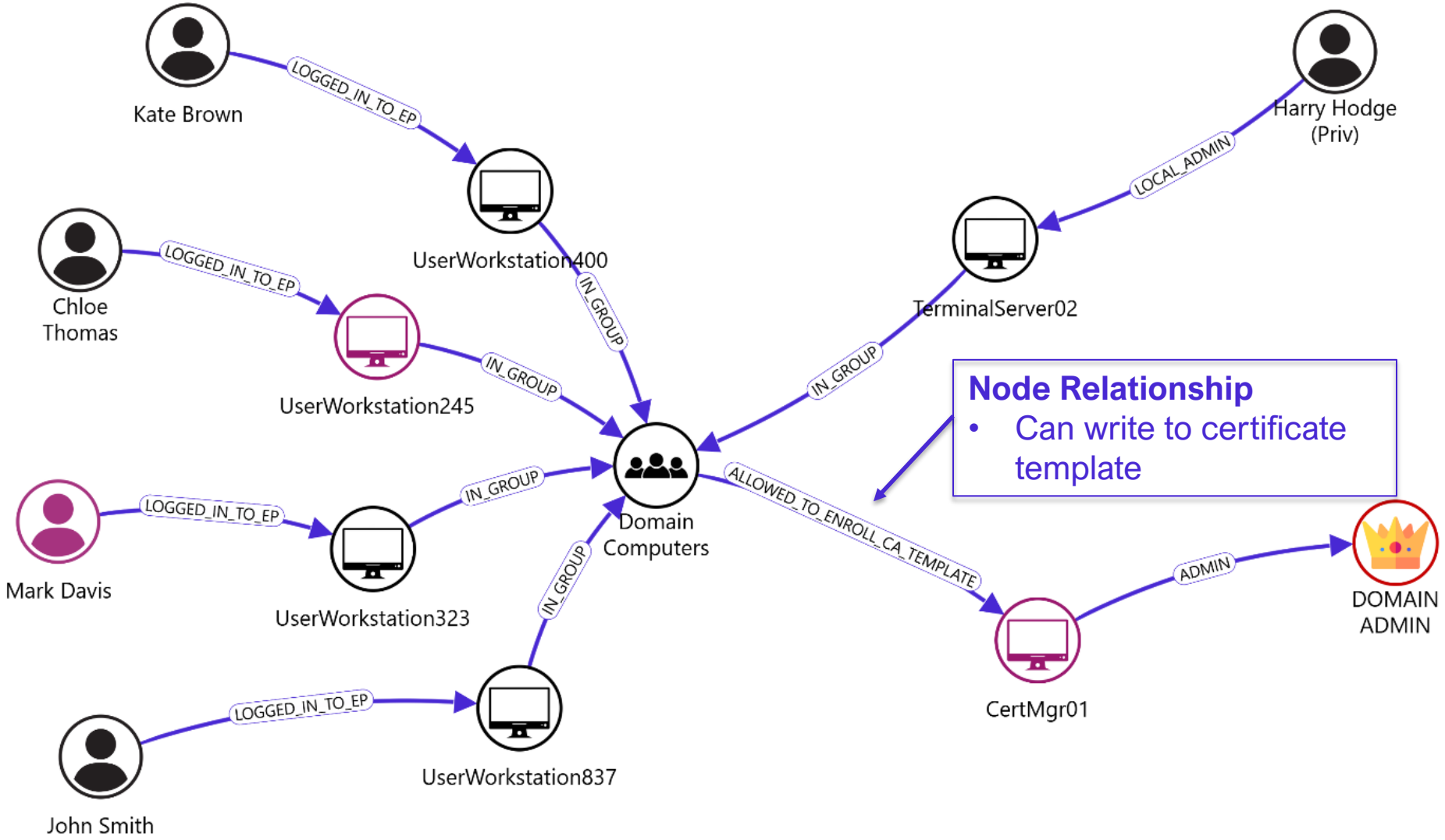
Use Case 2: The Stealthy Approach



NOTE: Data is simulated for presentation purposes

SA Power Networks

Use Case 3: Accidental Insider



NOTE: Data is ~~simulated~~ obfuscated for presentation purposes

SA Power Networks

What's next for our Attack Paths

- Bringing on additional data sources:
  - SharpHound (data collection for Active Directory environments)
  - Cloud resource identity permissions (e.g., Azure)
- Add additional risk mappings from data sources
  - Cloud misconfigurations
- Explore building the visualization with tools other than Power BI
  - BloodHound (evaluating and visualizing data collected by SharpHound)

RSAC 2025 Conference

Final Thoughts: Evolving our SOC Defenders

What We Learned

- Contextualizing from an attacker's lens has helped our SOC defenders think with a threat mindset
- Identifying most vulnerable entry points contextually has helped re-prioritize SOC activities for proactive response
- Risk remediation is now low effort, high impact and self-explanatory
- Understanding our technical and non-technical constraints from a blue team lens, prioritizes which critical path to remediate first
- Graphing our environment presents the big picture and real-time security posture changes

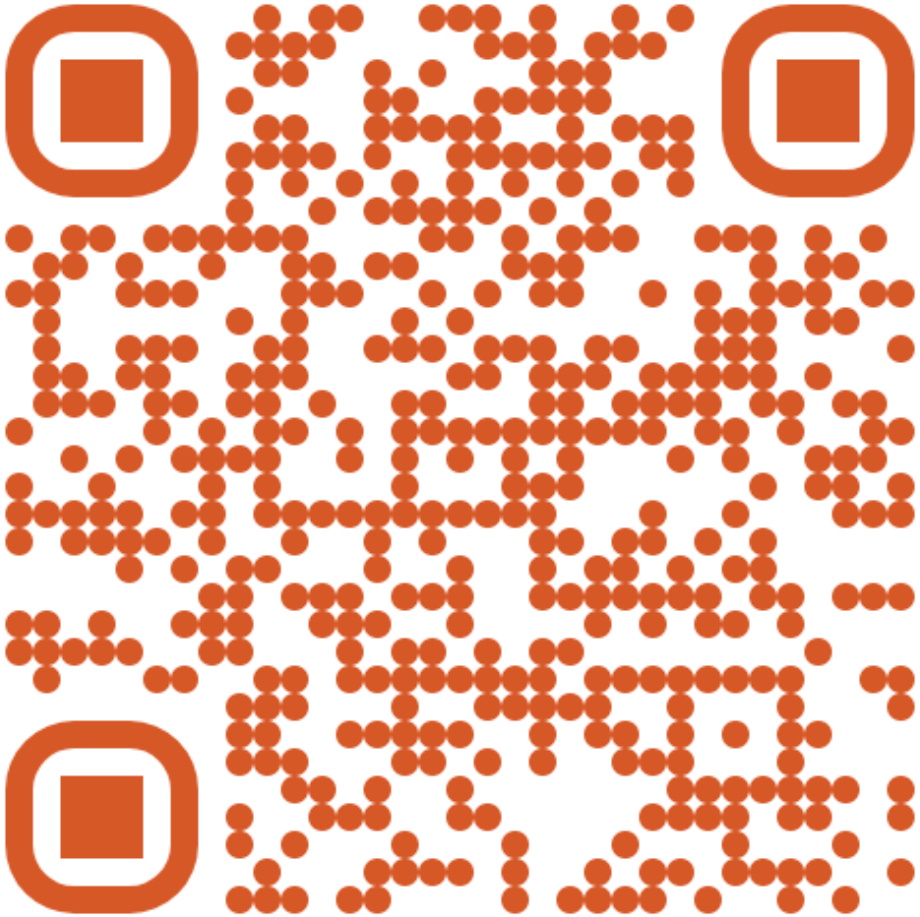
Apply What you learned today

- Next week you should:
  - Benchmark your SOC capability using Security Operations Maturity Model (SOMM)
  - Build a plan to remediate gaps in SOC people, process and technology
- In the first three months following this presentation you should:
  - Bring in data sources and develop a risk scoring criteria that is contextual to you
  - Build your first attack path model and align to a use case
- Within six months you should:
  - Be adopting and remediating attack paths as part of daily SOC operations
  - Tracking SOC metrics in remediating via attack paths vs previous method

Q&A

Attack Paths

Code and User Interface



RSAC 2025 Conference

Many Voices.
One Community.

Thank You

Lindbergh Caldeira

Ben Cooper